2020 EDITION

White Paper

UNDER ATTACK:
The Global Year in Breach

BTS TECHNOLOGIES

2020 EDITION

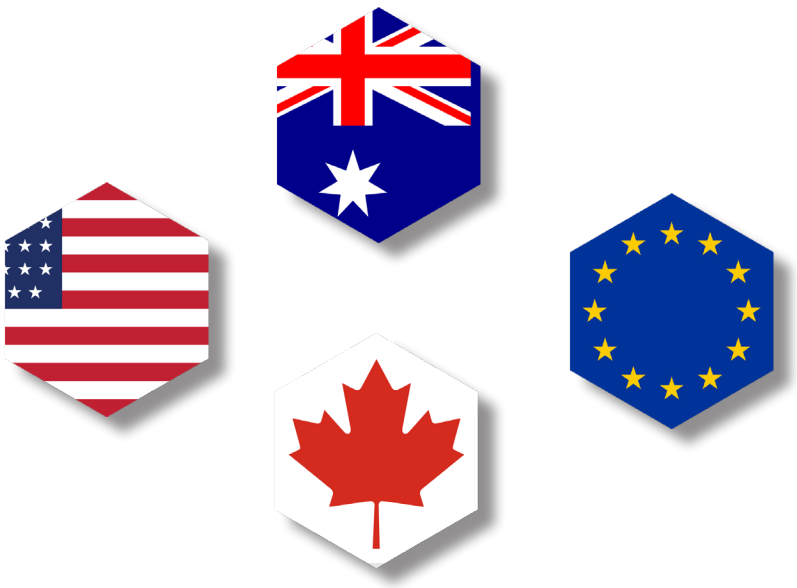
TABLE OF CONTENTS

FOREWARD

2019 was an interesting year for cybersecurity. Ransomware as a service, though around for a while now, really saw a sharp uptick in popularity. Numerous state and city governments were hit with malware. China allegedly hacked the phones of its Uyghur citizens, and hijacked both ASUS update servers and videogame developers to target specific Asian regions. We saw our first major GDPR fine when British Airways getting hit with $230 Million USD and the number of DDoS attacks increased by almost 1000%. Truly it was a great time to be around on the internet.

While the exact number of IoT devices reported in the world is surprisingly debated, or an inconsistently quoted number, at minimum by the end of the year Wi-Fi connected toasters will outnumber humans 4 to 1. In 2016, there was a DDoS attack that was more than one terabits per second, and with the expansion of the numbers of IoT devices along with the cringeworthy level of security applied to them, it seems increasingly likely we'll see a significantly larger DDoS attack in 2020.

2020 will also see the implementation of some new, American forms of GDPR-ish legislation. While obviously this will do little to decrease the rate at which breaches happen, it seems likely to decrease the amount of time companies take to notify people of breaches. Last year, popular online media company RoosterTeeth waited a full 10 days to notify users that their credit card information was stolen. This was one of the shortest periods of time between discovering and announcing breaches. Grocery store chain Hy-Vee waited two months to disclose that its credit card system had been infiltrated. With the pressure of additional laws mandating disclosure we should see these waiting periods get shorter.



SUMMARY

No matter which metrics you analyze, 2019 was a devastating time for data security. The year was a continuation of a disturbing trend that has produced ominous results in four key categories: cost, size, impact, and time. For instance, according to the Ponemon Institute's *2019 Cost of a Data Breach* study the cost of a data breach reached $3.92 million, an all-time high and 12% increase in just five years.

Cost **Size** **Impact** **Time**

At the same time, the average data breach compromised 25,575 records at an average cost of $150 each, a modest increase from 2018. However, the cost of a compromised record in the United States jumped considerably, reaching $242 per record, a $9 year-over-year increase.

While the healthcare industry was the most expensive sector when it came to data security, and understandably so, no industry was immune from the threat of a data breach. Notably, the financial consequences stemming from each breach were multifaceted, with customer turnover and decreased business capacity serving as the most significant contributors to losses.

THE AVERAGE TOTAL COST OF A BREACH INCREASED OVER 5 YEARS

$3.5 Million → 12% INCREASE → $3.92 Million

THE AVERAGE SIZE OF A DATA BREACH HAS INCREASED

24,615 records → 3.9% INCREASE → 25,575 records

THE AVERAGE TOTAL COST FOR EACH LOST RECORD INCREASED

$148 per Record → 1.4% INCREASE → $150 per Record

What's more, as every sector rushes to reap the benefits of digital transformation, they are also opening themselves up to increased risk. For instance, mobile technology is increasingly the target of various cybercrimes, as cybercriminals work to meet consumers on the platforms where they spend the most time.

Meanwhile, in 2019, the likelihood of experiencing a data breach has increased by 31% in just two years, and the life cycle increased by almost 5% since 2018 to a total of 279 days between detection and containment. At the same time, some companies were able to partner with security providers to adopt cybersecurity best practices and mitigate breaches. Designing and testing an incident response plan collectively **reduced the price tag by $680,000**, while employee training, encryption, and business continuity management also significantly reduced the cost of a breach. Around the world, companies are experiencing a lack of in-house resources to pursue these priorities. In total, 82% report a shortage of qualified cybersecurity professionals, a reality that is especially difficult for SMBs to navigate because they boast smaller cybersecurity budgets than mega-corporations.

This year, the threat landscape took another notable turn as consumers and privacy regulators began holding companies accountable for data security. This trend seems likely to continue as consumers are fleeing companies that can't protect their data, coupled with the introduction of new regulations, like California's Consumer Protection Act.

Follow along as the we explore the global landscape of data breaches across the United States, Canada, Europe, and Australia/New Zealand, providing you with actionable insights for protecting your customers and employees.

UNITED STATES

While large-scale, high profile data breaches continue to plague corporations, US breaches in 2019 were often targeted towards small companies and organizations, bringing significant consequences to their bottom lines. For example, more than 500 US schools were impacted by ransomware attacks, and 140 local governments experienced a 65% increase in these events. In total, it's estimated that ransomware attacks cost companies $7.5 billion in 2019.

At the same time, phishing scams reached unprecedented levels in regard to frequency and pervasiveness. According to Verizon's 2019 Data Breach Investigations Report, 32% of all data breaches began with a phishing attack. In the US, companies saw a 25% increase in the number of phishing scams that evaded their software defense, putting employee readiness at the top of many organization's to-do lists. In total, phishing scams account for the vast majority of data breaches, and an astonishing 76% of businesses reported being victimized by a phishing attack in the past year.

Both the increase in ransomware attacks and the prevalence of phishing scams reflect cybercriminals' desire to pursue soft targets that lack the resources or the resolve to adequately protect their IT infrastructure.

US COMPANIES SAW

25%

INCREASE IN THE NUMBER OF PHISHING SCAMS THAT EVADED THEIR SOFTWARE DEFENSE

TIMELINE OF US BREACHES IN 2019

February

EVITE

100M

Evite is one of the largest websites on the internet. However, they still didn't appropriately prioritize data security, as a hacker stole company data and placed it for sale on the Dark Web.

May

PERCEPTICS

100K

A security contractor endured a data breach that compromised images of travelers and license places crossing the Mexico/US border. The breach was costly for the company, which endured significant media scrutiny and was suspended from receiving federal contracts.

BALTIMORE, MD

N/A

A ransomware attack cost on the city of Baltimore cost more than $18 million to restore systems and recover lost revenue. While Baltimore is just one of many municipalities, educational institutions, and independent companies to be victimized in this way, it represents the incredible recovery costs associated with a ransomware attack.

June

QUEST DIAGNOSTICS

11.9M

In June, Quest Diagnostics identified a data breach that compromised customers' personally identifiable information and healthcare data. Aside from the sizeable scope of the breach, the episode was noteworthy because it underscores the cybersecurity vulnerabilities that arise from third-party partnerships, as dozens of companies experienced downstream data breaches due to the episode at Quest Diagnostics.

July

CAPITAL ONE

100M

A former Amazon Web Services software engineer hacked into Capital One's servers, ultimately compromising the personal information of 100 million people. The cybercriminal bragged about her activity online and left a trail of clues, indicating that she wanted to be identified. The episode was embarrassing and expensive for Capital One, costing the company as much as $150 million.

CANADA

In some respects, Canadian companies received some good news about the cost of a data breach in their region. Canada is the only country that experienced a net decrease in the average cost of a data breach, with the average expense of a compromised record reaching $187, a $15 year-over-year decline.

Canadians bear the burden of the third-highest cost of a data breach in the world, meaning that these escalating attacks will have serious financial consequences for organizations that are victimized by a breach.

AVERAGE PER RECORD COST = $150 PER RECORD

However, the reduced cost per record won't make a difference for many companies' bottom lines. According to a blog post by the Office of the Privacy Commissioner of Canada, the number of compromised records has increased six-fold since last year. In part, this is due to two large scale data breaches at Desjardins Group and Capital One that collectively compromised millions of records, but SMBs account for a growing number of data breaches as well. As the agency explains, "since reporting became mandatory, we've seen the number of data breach reports skyrocket. Some of those reports have involved well-known corporate names, but we have also seen significant volumes coming from small- and medium-sized businesses."

AVERAGE TIME TO IDENTIFY & CONTAIN A BREACH = 279 DAYS

AVERAGE NUMBER OF RECORDS COMPROMISED IN A BREACH = 25,575

AVERAGE DETECTION AND ESCALATION COSTS = $1.22M

EUROPE

In 2018, Europe set the global standard for data privacy when its General Data Protection Regulation (GDPR) went into effect on May 25th. This year, the financial implications of the law are being felt by businesses around the world. While prominent companies, including Marriott, British Airways, and Google, inspired a flurry of headlines when they received regulatory penalties, 27 companies incurred fines totaling €428,545,407.

As expected, the law significantly increased the number of reported data breaches, totaling more than 65,000 since its inception. The highest numbers are reported in the Netherlands, Germany, and the United Kingdom, which received 15,400; 12,600; and 10,600 breach notifications respectively.

€428

IN FINES FOR 27 COMPANIES WHO INCURRED REGULATORY PENALTIES

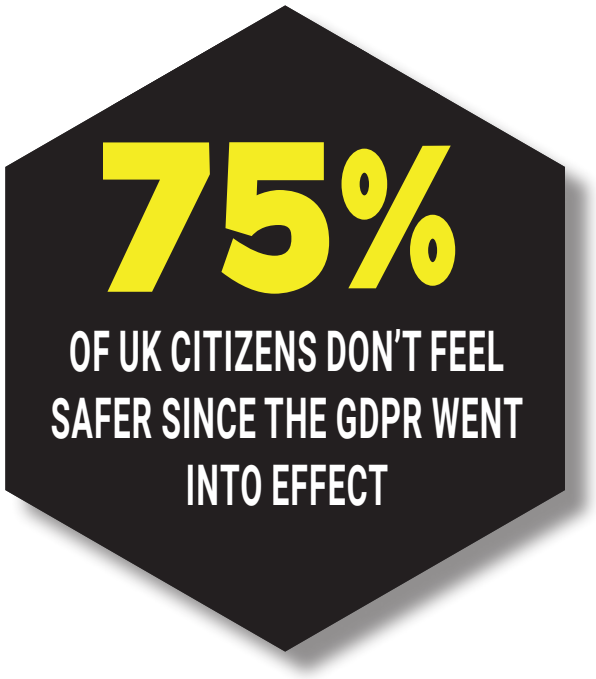
GDPR

While GDPR has brought significant attention to data privacy and so-called copycat laws that are being enacted by countries around the world, it has done little to quell consumers' fears about data security. As we reported last month, nearly three-quarters of UK citizens don't feel safer since the GDPR went into effect.

This a serious problem for businesses since it is coupled with the increasing tangible costs of a data breach, primarily driven by the financial penalties associated with privacy laws.

Unfortunately, UK SMBs are also struggling from a lack of available cybersecurity professionals and resources. In a survey conducted by the Department for Digital, Culture, Media, and Sport, found that the vast majority of SMBs do not have the right skills and experiences to effectively defend their digital environment.

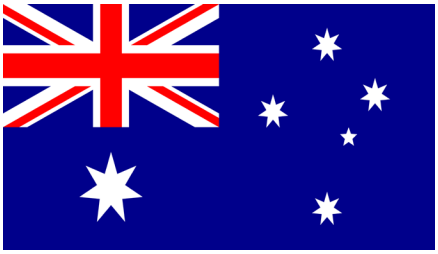
What's more, while GDPR imposed ominous penalties on companies that fail to protect customer data, the region continued to be plagued by security incidents.

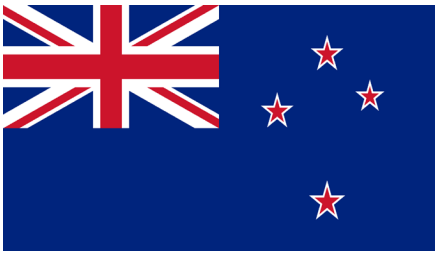


- Even government organizations aren't immune to the challenges of data security. The European Central Bank was forced to shut down one of its websites after it was infected with malware.

- Sonic Jobs inadvertently exposed the personal data for tens of thousands of job seekers when the platform failed to secure its cloud storage service.

- In August, a security researcher contacted a deluge of UK companies to assess their data subject access request procedures, a significant component of GDPR. 40% of organizations that responded to a phony information access request provided personal data to the researcher after he offered forged documents and without providing identity verification. The research didn't identify the noncompliant organizations, but it demonstrated the number of businesses struggling to comply with simple data compliance measures.





AUSTRALIA
NEW ZEALAND

Australians were significantly impacted by data breaches in 2019. Notably, an incident at the Office of the Australian Information Commissioner disclosed the personal details for more than 10 million people. With a population of just 25.4 million, this single episode accounts for a significant number of the country's population. Perhaps as a result, Australian consumers are increasingly skeptical of a company's data security standards, with 74% of Australian consumers indicating that a brand's data security is a significant factor when determining where and when to spend money.

Similarly, despite emerging privacy regulations in New Zealand, companies continue to experience data breaches at an alarming rate. More than a third of New Zealand businesses experienced a data breach in the past year, and many organizations still demonstrate a lack of understanding when it comes to the country's burgeoning regulatory standards.

For both countries, the cost of a data breach continues to be an enormous drag on both current and future earnings potential, meaning significant changes are likely underway at Australian and New Zealand businesses.

CONCLUSION

Around the world, data breaches became more prevalent, prolific, and expensive in 2019. While there are no signs that this trend will abate any time soon, it's clear that there is more that companies can do to protect their customer and company data. In this sense, growing regulatory oversight, abrasive customer responses, and escalating costs of recovery could be just the motivation that many businesses need to improve their defensive postures in the year ahead.

As 2019 reminds us, hackers most often rely on untrained, uninterested, and unaware employees to facilitate their crimes, and there is much than businesses of every size can do to defend against their schemes.

In today's digital-first landscape, a data breach can feel like an inevitability. However, those who understand the threat and position themselves to defend against the most prescient threats can win the battle for data security, an achievement that will pay substantial dividends now and in the years ahead.

As we head into 2021, we must do more to protect ourselves from data breaches. Call us today and save a future headache! (205) 290-8400

SOURCES

1. https://www.ibm.com/security/data-breach
2. https://info.idagent.com/blog/healthcare-and-the-dark-web
3. https://www.thesslstore.com/blog/the-top-cyber-security-trends-in-2019-and-what-to-expect-in-2020/
4. https://www.csis.org/analysis/cybersecurity-workforce-gap
5. https://info.idagent.com/blog/consumers-respond-to-data-privacy-regulations
6. https://www.zdnet.com/article/over-500-us-schools-were-hit-by-ransomware-in-2019/
7. https://www.govtech.com/blogs/lohrmann-on-cybersecurity/2019-the-year-ransomware-targeted-state--local-governments.html
8. https://www.crn.com/slide-shows/security/the-10-biggest-ransomware-attacks-of-2019
9. https://healthitsecurity.com/news/phishing-attacks-on-the-rise-25-increase-in-threats-evading-security
10. https://retruster.com/blog/2019-phishing-and-email-fraud-statistics.html
11. https://www.priv.gc.ca/en/blog/20191031/
12. https://www.bloomberg.com/news/articles/2019-06-20/desjardins-says-2-9-million-clients-exposed-in-quebec-data-leak
13. https://www.cnn.com/2019/07/29/business/capital-one-data-breach/index.html
14. https://alpin.io/blog/gdpr-fines-list/
15. https://blog.gemalto.com/security/2019/05/23/one-year-after-gdpr-significant-rise-on-data-breach-reporting-from-european-businesses/
16. https://info.idagent.com/blog/consumers-respond-to-data-privacy-regulations
17. https://which-50.com/fines-will-help-increase-the-cost-of-data-breaches-beyond-5-trillion-by-2024-juniper-research/
18. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/813599/Cyber_Security_Breaches_Survey_2019_-_Main_Report.pdf
19. https://www.itgovernance.co.uk/blog/40-of-organisations-respond-to-bogus-dsars?utm_source=blog
20. https://uk.reuters.com/article/us-ecb-cyber/ecb-shuts-down-one-of-its-websites-after-hacker-attack-idUKKCN1V51N0
21. https://www.computerworld.com/article/3412255/the-most-significant-data-breaches.html
22. https://www.zdnet.com/article/over-10-million-people-hit-in-single-australian-data-breach-oaic/
23. https://securityboulevard.com/2019/07/trust-is-a-must-for-wary-australian-consumers-new-study-reveals-data-security-influences-purchasing-habits/
24. https://www.scoop.co.nz/stories/BU1911/S00500/the-cyber-security-war-how-nz-businesses-are-affected.htm

REPRINTED WITH PERMISSION FROM ID AGENT